Käyttäjähallinnon vähimmäisvaatimukset ja soveltamisohjeet

Dokumentin tarkoitus

Tämä dokumentti on Haka-luottamusverkoston operaattorin tekemä tulkintaohje Haka-liittymissopimukselle ja sen liitteessä 3. esitetyille, kotiorganisaatiota koskeville vaatimuksille. Lisäksi dokumentissa täsmennetään joitain liitteessä määriteltyjä asioita sekä funetEduPerson-skeeman käyttöä.

Dokumentin päämäärä on esittää operaattorin toimintalinja kotiorganisaation sisäisen käyttäjähallinnon arvioinnissa ja taata korkeakoulujen tasapuolinen kohtelu.

Dokumentin kohderyhmä

- korkeakoulussa käyttäjähallinnosta vastaavat tahot (it-keskus tai vastaava)
- palveluntarjoajat

Tulkintaohjeet

1. Tulkinta: käyttäjätietojen ajantasaisuus

Tausta:

- Yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan d alakohta: "*henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä; on toteutettava kaikki mahdolliset kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä (”täsmällisyys”);*" Lisäksi, 5 artiklan 2 kohta: "*Rekisterinpitäjä vastaa siitä, ja sen on pystyttävä osoittamaan se, että 1 kohtaa on noudatettu (”osoitusvelvollisuus”).*"
- Haka-palvelusopimus, liite 3, kohta 2.3.6: *"Kotiorganisaatiot varmistavat asiaankuuluvaa huolellisuutta noudattaen, että vain virheettömiä ja ajantasaisia (...) henkilötietoja luovutetaan palveluntarjoajille"*
- Haka-ohjausryhmän tulkinta 26.5.2004: *"Tieto käyttäjän käyttöoikeuden päättymisestä tulee päivittyä mielellään välittömästi, kuitenkin viimeistään viikon sisällä, sisältäen mahdollisen armonajan (grace). Käytännössä tämä edellyttää käyttäjähallinnon kytkemistä organisaation perusrekistereihin, kuten opiskelija- ja henkilökuntarekisteriin."*

Tulkinta/ajantasaisuus:

- Kotiorganisaation Identity Provider (IdP) -palvelin voidaan kyllä rekisteröidä Haka-infrastruktuuriin, mutta se saa **tarjota käyttäjistä vain sellaisia attribuutteja, jotka ovat ajan tasalla** IdP:n käyttämässä käyttäjätietokannassa. Jos esimerkiksi käyttäjätietokannan ja opiskelijarekisterin väliltä puuttuu kytkentä, ei IdP saa tarjota Haka-infrastruktuuriin käyttäjien opiskelijaroolia koskevia attribuutteja (esim. koulutusohjelma, tavoitetutkinto tai eduPersonAffiliation=student)
    - Haka-palvelusopimuksen liitten 3 kohdan 2.3.5. mukaan kuitenkin vähintään funetEduPerson-skeeman MUST-attribuuteille on annettava arvo; niitä ovat skeman versiossa 2.0 common name, surname, displayName, eduPersonPrincipalName, schacHomeOrganization, schacHomeOrganizationType, joista kaksi jälkimmäistä lienevät samat kaikillä käyttäjille IdP:ssä
    - Palveluntarjoajan ei ole syytä olettaa, että pelkkä "shibboleth-tunnistamisen onnistuminen" takaisi mitään muuta kuin että henkilöllä on käyttäjätunnus kyseisessä organisaatiossa. Jotkut korkeakoulut voivat antaa käyttäjätunnuksia alumneille, emerituksille tai kirjaston asiakkaina oleville "kadunmiehille".
    - Toisaalta: palveluntarjoaja voi vaatia kotiorganisaatiolta palvelun kannalta tarpeellisia attribuutteja (esim. eduPersonAffiliation=student) käyttöoikeuksien toteamista varten. Kotiorganisaatio, joka ei voi tarjota palvelun vaatimia attribuuttia, rajautuu ulos kyseisestä palvelusta.

Tulkinta/perusrekisterikytkentä:

- kytkentä organisaation perusrekistereihin voi olla **joko tekninen** (esim. skripti välittää perusrekisterin muutokset käyttäjätietokantaan) **tai perustua organisaation toimintaprosesseihin** (esim. opintoasiainhallinnon virkailija sulkee opiskelijan käyttäjätunnuksen samalla kun opiskelija tulee hakemaan tutkintotodistusta, tai päivittää opiskelijan ilmoittaman muuttuneen kotiosoitteen paitsi opiskelijarekisteriin, myös käyttäjätietokantaan). Jos käyttäjätunnuksen sulkeutuminen taataan toimintaprosessin avulla, tulee toimintaprosessin olla määrämuotoinen ja dokumentoitu, ja sitä tulee myös tosiasiallisesti noudattaa.
- jos käyttäjällä ei ole organisaatiossa perusrekisteriä (esim. Suomen Akatemian palkkaama tutkija, joka työskentelee tutkimusryhmässä yliopiston laitoksella), tulee kotiorganisaation taata käyttäjän käyttäjätunnuksen tai roolitiedon sulkeutuminen äärellisessä ajassa tekemällä siitä **määräaikain en**.

Rajaus:

- nämä vaatimukset koskevat vain Haka-infrastruktuurin palveluntarjoajien suuntaan näkyvää toimintaa. Haka-infrastruktuuri ei ota kantaa siihen, koska esimerkiksi organisaatiosta poistuvien henkilöiden **organisaation sisäiset käyttäjätunnukset** (esim. Unix tai sähköposti) sulkeutuvat.
- Haka-infrastruktuurin tehtävä ei ole ottaa kantaa siihen, koska korkeakoulu **tulkitsee että opiskelija lakkaa olemasta opiskelija** (ja hänen oikeutensa opiskelijoille tarkoitettuihin resursseihin päättyy). Jonkun korkeakoulun mukaan tämä tapahtuu valmistumishetkellä, toisen korkeakoulun mukaan tämä tapahtuu kun valmistumishetkellä kulumassa oleva lukuvuosi päättyy.
- Tyypillisesti korkeakouluissa on myös lukukausi-ilmoittautumisajan päättymisen aikaan ylimenovaihe, jolloin sekä päättyvälle että alkavalle lukukaudelle ilmoittautuneet opiskelijat ovat Haka-näkökulmasta opiskelijoita.

2. Tulkinta: henkilöllisyyden todentaminen käyttäjätunnusta annettaessa

- Haka-liittymissopimus, liite 3, 2.3.2: *"Antaessaan käyttäjätunnuksen uudelle loppukäyttäjälle kotiorganisaatio todentaa käyttäjätunnuksen saajan henkilöllisyyden luottamusverkoston toimintakäytäntöjen mukaisesti sekä vaatii, että käyttäjä hyväksyy ja sitoutuu noudattamaan kotiorganisaationsa käyttösääntöjä."*

Haka-luottamusverkoston ensitunnistuskäytäntö vastaa vähintään IAP/low arvoa. Katso alla olevasta taulukosta soveltuvat menetelmät. Poikkeukset käytäntöön kuvataan jäsenen käyttäjähallintokuvauksessa.

Käytetty ensitunnistustaso viestitään pakollisessa eduPersonAssurance attribuutissa. eduPersonAssurance attribuutin arvot noudattavat REFEDS tunnistuksen varmuuden viitekehystä. Arvot kumuloituvat, ts. medium -tasolla attribuutin arvoiksi asetetaan sekä $PREFIX/IAP/low että $PREFIX/IAP /medium. Vastaavasti high -tasolla $PREFIX/IAP/low, $PREFIX/IAP/medium ja $PREFIX/IAP/high.

eduPersonAssurance arvo, $PREFIX=https://refeds.org/assurance	**Kuvaus ja tulkinta soveltuvista menetelmistä**
`$PREFIX$/IAP/low`	Identity proofing and credential issuance, renewal, and replacement qualify to any of • sections 5.1.2-5.1.2.9 and section 5.1.3 of Kantara assurance level 1 [Kantara SAC] • IGTF level DOGWOOD [IGTF] • IGTF level ASPEN [IGTF] Example: self-asserted identity together with verified e-mail address, following sections sections 5.1.2-5.1.2.9 and section 5.1.3 of [Kantara SAC].
	Tulkinta soveltuvista menetelmistä (1.2.2022 jälkeen): • Erikseen rekisteröity (opintohakemus tms.), varmistettu sähköpostiosoite
`$PREFIX$/IAP/medium`	Identity proofing and credential issuance, renewal, and replacement qualify to any of • sections 5.2.2-5.2.2.9, section 5.2.2.12 and section 5.2.3 of Kantara assurance level 2 [Kantara SAC] • IGTF level BIRCH [IGTF] • IGTF level CEDAR [IGTF] • section 2.1.2, section 2.2.2 and section 2.2.4 of eIDAS assurance level low [eIDAS LoA] Example: the person has sent a copy of their government issued photo-ID to the CSP and the CSP has had a remote live video conversation with them, as defined by [IGTF].
	Tulkinta soveltuvista menetelmistä: • Kasvotusten kuvallisesta paikallisviranomaisen myöntämästä virallisesta henkilöllisyystodistuksesta Mikäli edellä kuvatut eivät ole mahdollisia tunnistustapoja voidaan tunnistaminen toteuttaa: • eduGAIN-kirjautuminen, mikäli voidaan varmistaa ja dokumentoidaan, että kyseisen organisaation ensitunnistamisen vahvuus on vähintään samaa tasoa • Kirjatun kirjeen avulla, jolloin tunnistus tapahtuu postissa kuvallisesta henkilöllisyystodistuksesta • Luotettu henkilö tunnistaa käyttäjän kuvallisesta virallisesta henkilötodistuksesta, samoin periaattein, kuin käyttäjä tunnistettaisiin paikan päällä organisaatiossa • Videolinkin yli kuvallisesta henkilöllisyystodistuksesta [IGTF] [EUGridPMA]
`$PREFIX$/IAP/high`	Identity proofing and credential issuance, renewal, and replacement qualifies to any of • section 5.3.2-5.3.2.9, section 5.3.2.12 and 5.3.3 of Kantara assurance level 3 [Kantara SAC] • section 2.1.2, section 2.2.2 and section 2.2.4 of eIDAS assurance level substantial [eIDAS LoA] Example: the person has presented an identity document that is checked to be genuine and represent the claimed identity and steps have been taken to minimise the risk of a lost, stolen, suspended, revoked or expired document, following sections 2.1.2, 2.2.2 and 2.2.4 of eIDAS assurance level substantial [eIDAS LoA].
	Tulkinta soveltuvista menetelmistä: • Vahva sähköinen tunnistus: suomi.fi tai Eidas-tunnistamisen korotettu tai korkea luotettavuustaso • Kasvotusten kuvallisesta paikallisviranomaisen myöntämästä virallisesta henkilöllisyystodistuksesta ja tarkistetaan ettei todistus ole ilmoitettu hukkuneeksi, varastetuksi tai lakkautetuksi.

[KANTARA-SAC] https://kantarainitiative.org/download/7663/

[IGTF] https://www.igtf.net/ap/authn-assurance/

[eIDAS LoA] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0002

[EUGridPMA] http://wiki.eugridpma.org/Main/VettingModelGuidelines

3. Täsmennettyjä ohjeita skeemasta

- funetEduPerson-skeeman on tarkoitus olla yhteinen nimittäjä Haka-infrastruktuurissa siirrettäville attribuuteille. Kotikorkeakoulut ja palveluntarjoajat voivat sopia myös muista attribuuteista.

3.1.Yksilöivä tunniste (eduPersonPrincipalName,EPPN)

- Käyttäjän yksilöivänä tunnisteena käytetään eduPersonPrincipalName -attribuuttia (muotoa xxxxxx@domain, esim. linden@tut.fi)
- Domain-nimenä käytetään korkeakoulun domain-nimeä
  - suositus: sama korkeakoulu ei käyttä attribuutissa eri domain-nimiä, esimerkiksi yliopisto.fi ja staff.yliopisto.fi
- on kotikorkeakoulun sisäinen asia,minkä arvon domain-spesifi osa saa
  - arvo voidaan ottaa esimerkiksi käyttäjätunnuksesta (esim. linden@tut.fi)
- yhdellä tosielämän henkilöllä voi olla **useita EPPN-attribuutteja**
  - erityisesti: eri attribuutti kotikorkeakoulussa opiskelija- ja henkilökuntarooleihin (amk:ssa tyypillisesti opiskelija-työntekijällä kaksi käyttäjätunnusta)
  - lisäksi: tosielämän henkilöllä, joka esimerkiksi opiskelee kahdessa korkeakoulussa, on kaksi EPPN-tunnistetta (esim. eskoesim@korkeakoulu-a.fi ja eesimerk@korkeakoulu-b.fi)
  - tällöin loppukäyttäjän on kirjautuessa palveluun lähtökohtaisesti itse tiedettävä, minä näistä esiintyy
  - palveluntarjoajan tulee huomioida tämän vaikutukset palvelua rakentaessaan
- henkilön EPPN-attribuutti saa **vaihtua vain painavista syistä**
  - painava syy saattaa olla esimerkiksi avioero, jolloin sukunimen sisältävää domain-spesifiä osaa voidaan muuttaa
  - jos käyttäjä haluaa profiilitietonsa säilyvän käyttämissään palveluissa, voi käyttäjä pyytää kotikorkeakouluaan ilmoittamaan EPPN-tunnisteen muuttumisesta palveluntarjoajalle
- henkilön EPPN-attribuutin **kierrättäminen**
  - kotiorganisaation tulee huolehtia, että samaa EPPN-attribuutin arvoa ei anneta eri henkilölle. Kotiorganisaatio voi harkita, antaako saman EPPN-attribuutin arvon samalle henkilölle uudelleen myöhemmin vai antaako henkilölle uuden EPPN-attribuutin arvon.

3.2. Henkilötunnus (schacPersonalUniqueID)

- korkeakoulu on voinut antaa käyttäjälle, jota ei ole kirjattu väestötietojärjestelmään, sisäiseen käyttöön tarkoitetun "keinotekoisen" henkilötunnuksen
- kotiorganisaatio **ei saa asettaa keinotekoista henkilötunnusta schacPersonalUniqueID-attribuutin** arvoksi
  - koska mikään ei takaa, että *joku toinen* organisaatio ei ole antanut samaa henkilötunnusta eri henkilölle

3.3. Kotiorganisaatio (schacHomeOrganisation)

- kotiorganisaation tulee antaa **jokaiselle loppukäyttäjälle sama arvo**

3.4. Tunnistuksen varmuus (eduPersonAssurance)

Haka-liittymissopimuksen, tämän dokumentin ja REFEDS Assurance Frameworkin vaatimuksien täyttyessä kotiorganisaatiot voivat luovuttaa eduPersonAssurance attribuutin arvoina

- https://refeds.org/assurance/ID/eppn-unique-no-reassign
- https://refeds.org/assurance/ATP/ePA-1m
- https://refeds.org/assurance/IAP/medium
- https://refeds.org/assurance/IAP/low
- https://refeds.org/assurance

Alla olevassa taulukossa on eduPersonAffiliation arvojen vastaavuus moniarvoisen eduPersonAssurance attribuutin arvoihin 1.1.2021 alkaen. Taulukko vastaa tämän hetkistä käytäntöä. Esimerkiksi tutkinto-opiskelija on ensitunnistettu kohdan 2. taulukon mukaisesti, kirjautumistapahtumassa eduPersonAssurance tulisi sisältää kyseiselle tutkinto-opiskelijalle vähintään 'https://refeds.org/assurance/IAP/medium' ja 'https://refeds.org/assurance/IAP/low' arvot.

eduPersonAffiliation	**eduPersonAssurance** **$PREFIX=https://refeds.org/assurance**
student	$PREFIX/IAP/medium, $PREFIX/IAP/low
faculty	$PREFIX/IAP/medium, $PREFIX/IAP/low
staff	$PREFIX/IAP/medium, $PREFIX/IAP/low
employee	$PREFIX/IAP/medium, $PREFIX/IAP/low
member	$PREFIX/IAP/medium, $PREFIX/IAP/low
affiliate	$PREFIX/IAP/medium, $PREFIX/IAP/low
alum	$PREFIX/IAP/medium, $PREFIX/IAP/low

library-walk-in	$PREFIX/IAP/medium, $PREFIX/IAP/low

4. Tulkinta: tietojen edelleen luovuttaminen

- Haka-liittymissopimus, kohta: "8. Palveluntarjoajan oikeudet ja velvollisuudet":
  - "ei saa käyttää saamiaan henkilötietoja muihin tarkoituksiin kuin mitä palvelua koskevassa Tietosuojailmoituksessa on määritelty."

Tulkinta:

- Haka-kirjautumisesta saatujen tietojen edelleen luovuttaminen voi tapahtua kahden Haka-palvelun välillä, kun molemmat palvelut ovat Hakan jäseniä ja ovat näin ollen Haka-sopimuksella sitoutuneet noudattamaan Haka-sopimuksen velvoitteita. Lisäksi henkilötietoa koskevaa henkilöä on informoitu tietojen luovuttamisesta ja luovutettavien tietojen käyttötarkoitus on yhteensopiva luovutuksen kohteena olevassa palvelussa.

Versiohistoria

Päiväys	Muutos
8.2.2005	Dokumentti luotu; pohjana Haka-infrastruktuurin ohjausryhmän päätökset, joita ei ole sisällytetty itse HAKA-palvelusopimukseen
15.2.2005	Ohjausryhmä: henkilötietojen poisto 18->15 kk
22.6.2006	funetEduPerson 2.0:n aiheuttamat muutokset (mm. uudet schac-attribuutit, vaihtuneet MUST-attribuutit). EPPN-kierrätysajan venytys 24 kk :een ja uusi EPPNTimeStamp-attribuutti. Opiskelijaroolin säilymiskäytäntö lukukausi-ilmoittautumisen aikana tuotu erikseen esiin.
28.8.2013	Lisätty tulkinta: "tietojen edelleen luovuttaminen", josta ohjausryhmä on päättänyt 17.5.2013 kokouksessa 1-2013
10.10.2017	Päivitetty 2. kohdan tulkintaa ensitunnistamisesta tilanteessa, jossa käyttäjää ei tavata henkilökohtaisesti tai suomalaisen vahvan tunnistamisen menetelmillä. Käsitelty Haka-ohjausryhmän kokouksessa 2/2017 ja IAM-verkoston tapaamisessa 10.10.2017
21.1.2020	Päivitetty "käyttäjätietojen ajantasaisuus" tausta viittaamaan tietosuoja-asetukseen ja poistettu tulkinta "siirtymäaika" vanhaan palvelusopimukseen liittyneistä siirtymäajoista.
29.6.2020	Lisätty eduPersonAssurance attribuutin REFEDS Assurance Frameworkin (RAF) mukaisista arvoista
21.10.2020	Tarkennettu RAF ensitunnistuslähtötasoksi IAP/medium luottamusverkoston ensitunnistusvaatimuksien pysyessä samana.
31.3.2021	Päivitetty 2. kohdan kuvaus ja tulkinta soveltuvista ensitunnistusmenetelmistä
2.2.2022	Päivitetty Hakan ensitunnistuksen vähimmistaso arvoon IAP/low